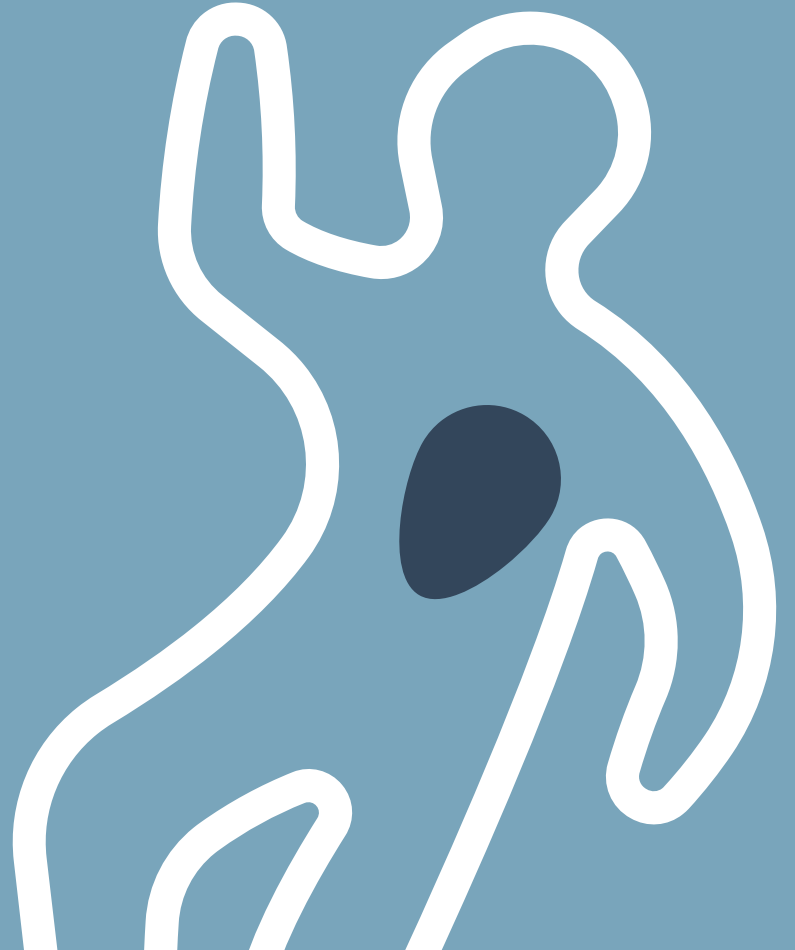




DIGITAL FORENSICS

Manahil Masroor & Komal Kaler



03

Identification, Evidence Collection,
Analysis, Documentation, Reporting

02 ACPO PRINCIPLES

What They Are & 4
Principles

01 DIGITAL FORENSICS

Definition, Uses, Types of Crimes, Example
of Cases that used Digital Forensics

04 ANTI-FORENSICS

Encryption, Password Attacks,
Steganography, Data Destruction

05 THE FUTURE

Cloud Forensics, SSD &
NAND

TABLE OF CONTENTS





FORENSICS SCIENCES

Scientific test or techniques involved with the detection of crime.



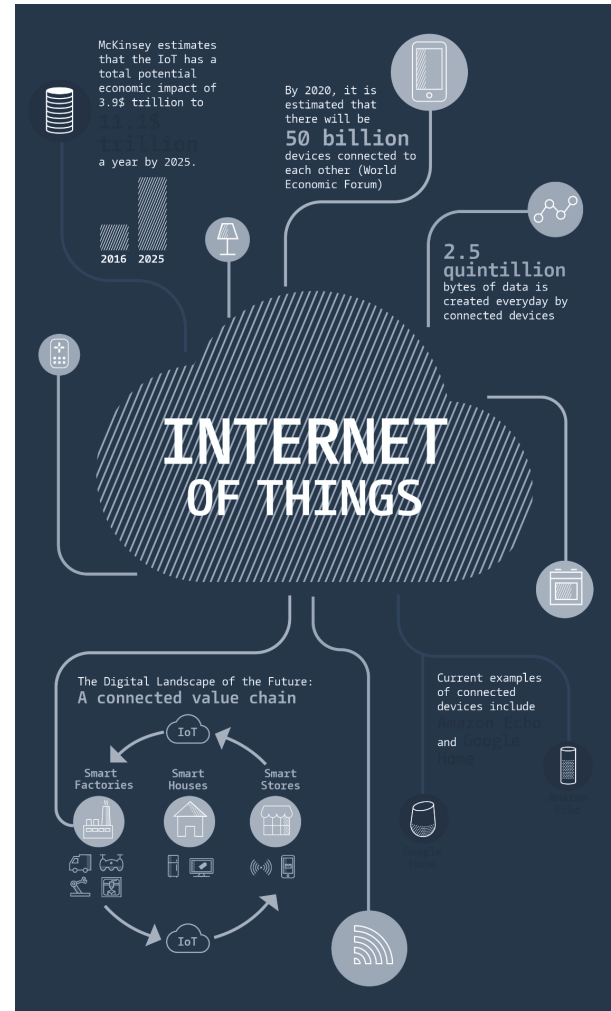
DIGITAL FORENSICS

The use of analytical and investigative techniques to identify, collect, examine and preserve evidence.



Digitalization of the World

- **NOT JUST COMPUTERS**
 - ATMS
 - Phones
 - Smart Watches
 - pOS
 - Cameras
 - Smart Lights
 - Smart Washers
 - Smart Thermostats
 - Smart Locks
 - Smart Home Devices
 - Smart Cars
- **Anything That Can Be Connected to the Internet**



Digitized Crime

COMPUTER FACILITATED CRIME

Computer as a tool.

Evidence is on computer or computer was used in criminal activity.

Ex. Child Pornography, criminating emails etc.



COMPUTER BASED CRIME

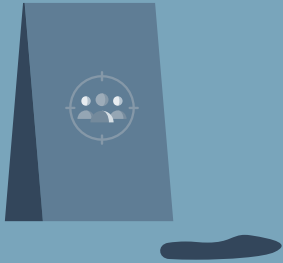
Computer as a target.

Computer was used to target other computer or network based crime.

Ex. Ransomware, Hacking etc.

WHEN TO USE DIGITAL FORENSICS

Criminal Investigations



Civil Litigation



Intelligence



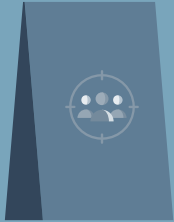
Administrative



WHEN TO USE DIGITAL FORENSICS

**Our
Focus**

Criminal Investigations



Civil Litigation



Intelligence



Administrative



The Craigslist Killer (mobile and email)

- Used Craigslist to find victims acting as a customer
- FBI traced the emails exchanged between the victims to the killer and found his IP address
- Subpoenaed Facebook for his account information and got trailed him to get fingerprints that would place him at the crime
- Interrogation
- Computer as tool crime



The BTK Killer (Hard Drive Metadata)

- Took over 30 years to solve
- From 1974 and 1991, Tortured and killed over 10 people and left notes to taunt the police
- Jan 2005, Sent a floppy disk with pictures and videos of his killings and a microsoft doc
- Scoured the metadata contained within the disk to find 2 things:
 - A church (**Christ Lutheran Church**)
 - A first name (**Dennis**)
- Feb 2005, arrested after matching fingerprints from his car
- Computer as a tool crime



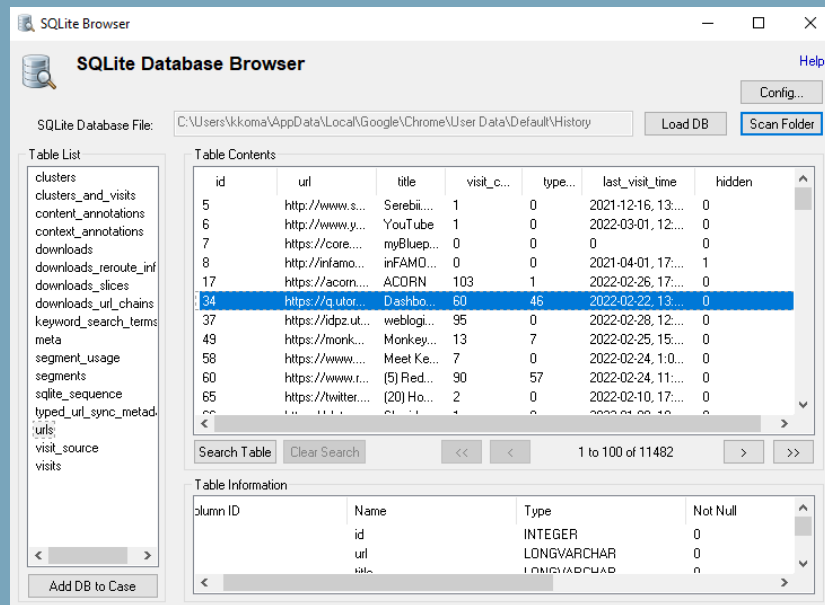
4.5 Billion BTC Heist (Email and Blockchain)

- Stole 4.5 Billion from Bitfinex in 2011, was unsolved for 11 years
- May 3, 2020, some of the BTC was transferred and sold in a crypto exchange that sells prepaid cards
- \$500 gift card for Walmart was sent to a Russian-registered email and redeemed through Walmart's phone app.
- Online orders were under Ms. Morgan's name, using one of her emails, and the couple's apartment address
- Computer as a tool and a target crime



Browser Forensics (Try on Your Own Time!)

- OSForensics is a popular tool used
- \Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\ (Google Chrome, Windows)
- \Users\%userprofile%\Library\Safari (Safari, MacOS)
- These folders contain
 - History
 - Cache
 - Cookies
 - Typed URLs
 - Sessions
 - Most visited sites
 - Screenshots
 - Financial info
 - Form values (Searches, Autofill)
 - Downloaded files (Downloads)
 - Favorites



The screenshot shows the SQLite Database Browser interface. The SQLite Database File is set to C:\Users\kkoma\AppData\Local\Google\Chrome\User Data\Default\History. The Table List on the left includes various browser data tables. The Table Contents pane displays a table with columns: id, url, title, visit_c..., type..., last_visit_time, and hidden. The table contains 10 rows of data, with the row for id 34 highlighted. The Table Information pane at the bottom shows the schema for the selected table.

id	url	title	visit_c...	type...	last_visit_time	hidden
5	http://www.s...	Serebi...	1	0	2021-12-16, 13:...	0
6	http://www.y...	YouTube	1	0	2022-03-01, 12:...	0
7	https://core....	myBluep...	0	0	0	0
8	http://infamo...	inFAMO...	0	0	2021-04-01, 17:...	1
17	https://acom....	ACORN	103	1	2022-02-26, 17:...	0
34	https://q.utor...	Dashbo...	60	46	2022-02-22, 13:...	0
37	https://idpz.ut...	weblogi...	95	0	2022-02-28, 12:...	0
49	https://monk...	Monkey...	13	7	2022-02-25, 15:...	0
58	https://www....	Meet Ke...	7	0	2022-02-24, 1:0...	0
60	https://www.t...	(5) Red...	90	57	2022-02-24, 11:...	0
65	https://twitter...	(20) Ho...	2	0	2022-02-10, 17:...	0

column ID	Name	Type	Not Null
1	id	INTEGER	0
2	url	LONGVARCHAR	0
3	tit...	LONGVARCHAR	0

ACPO 4 Principles

1. Evidence Tampering



No action taken by law enforcement agencies or agents should change data held on a computer or storage media which may subsequently be relied upon in court.

2. Accountability & Responsibility



If necessary to access original data held on storage or device, person must be qualified to do so and able to give evidence explaining the relevance and implications their actions.



3. Chain of Custody

An audit trail or record of all processes applied to electronic evidence should be created and preserved. An independent 3rd party should be able to examine those processes and achieve the same result.

4. Case Officer Responsibility



The person in charge of the investigation (case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

The Digital Forensics Process



Identification	Crime Scene & First Response, Search and Seizure
Evidence Collection & Preservation	Acquisition & Imaging, Live vs Dead Imaging, Hash Analysis
Analysis	Timestamps, File Metadata, Windows Registry
Documentation & Reporting	Chain of Custody, Final Reports & Expert Witness

The Digital Forensics Process



Identification	Crime Scene & First Response, Search and Seizure
Evidence Collection & Preservation	Acquisition & Imaging, Live vs Dead Imaging, Hash Analysis
Analysis	Timestamps, File Metadata, Windows Registry
Documentation & Reporting	Chain of Custody, Final Reports & Expert Witness

DO NOT CROSS

First Response & The Crime Scene

1. Safety
2. Removal of people & devices
3. Document (or photograph) the scene
4. Course of Action
5. Seize or Image
6. Disconnect from Network
7. Search Scene for evidence



DO NOT CROSS

Go Kit

- Labels and Stickers
- Cable Ties
- Anti-Static Gear
- Adapters and cables (different sizes)
- A write blocker
- Gloves
- Screwdriver
- Flashlight
- External Storage
- Chain of custody doc
- Digital camera
- Recording tools (notebook, pen, digital and recorder)
- Brown Paper evidence bag
- Manila Folders
- Evidence Tags
- Scissors
- Evidence/ packaging tape
- Imaging Devices
- Dongles
- Triaging programs



Search Laws in Canada

From Section 8 of the Charter of Rights:

“Everyone has the right to be secure against unreasonable search or seizure.”

1. Has there been a search and seizure?

- an examination of the subject matter of the search
- a determination as to whether the claimant had a direct interest in the subject matter
- an inquiry into whether the claimant had a subjective expectation of privacy in the subject matter
- an assessment as to whether this subjective expectation of privacy was objectively reasonable

Search Laws in Canada

From Section 8 of the Charter of Rights:

“Everyone has the right to be secure against unreasonable search or seizure.”

2. What does it mean to be a reasonable search?

- The search is authorized by law
 - Warrant vs Warrantless
- The law itself is reasonable
 - No hard test to determine
- The manner in which the search is carried out is reasonable
 - Must identify before breaking in

- Traditional vs Digital crime scene
- Don't change the status of the device
 - Which status is preferred? Live or Dead
- Don't operate it
- Take pictures
- Faraday Bag



The Digital Forensics Process



Identification	Crime Scene & First Response, Search and Seizure
Evidence Collection & Preservation	Acquisition & Imaging, Live vs Dead Imaging, Hash Analysis
Analysis	Timestamps, File Metadata, Windows Registry
Documentation & Reporting	Chain of Custody, Final Reports & Expert Witness

ACQUISITION & PRESERVATION

Cloning

Data is cloned and copied from original electronic source.

Hashing

To verify any changes in evidence or content.

Live System vs
Dead System

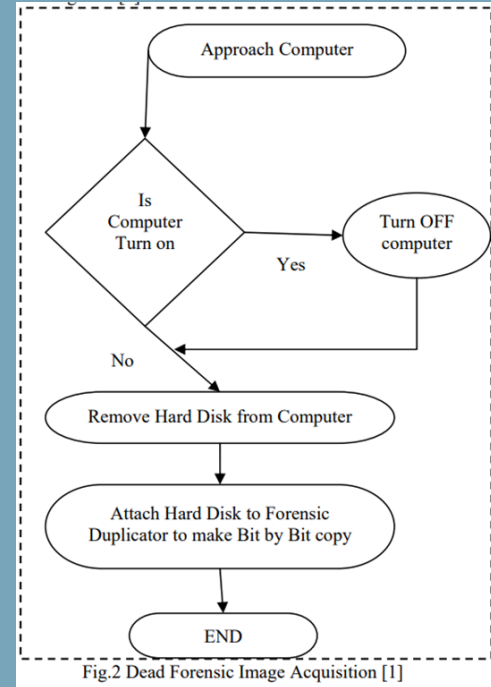
Imaging

Powered On vs Powered
Off: Which one is better?

Imaging: Cloning/copying a physical storage for gathering evidence.
Pulling the plug was preferred but now is now subject to debate.

DEAD SYSTEMS aka Powered off Machines:

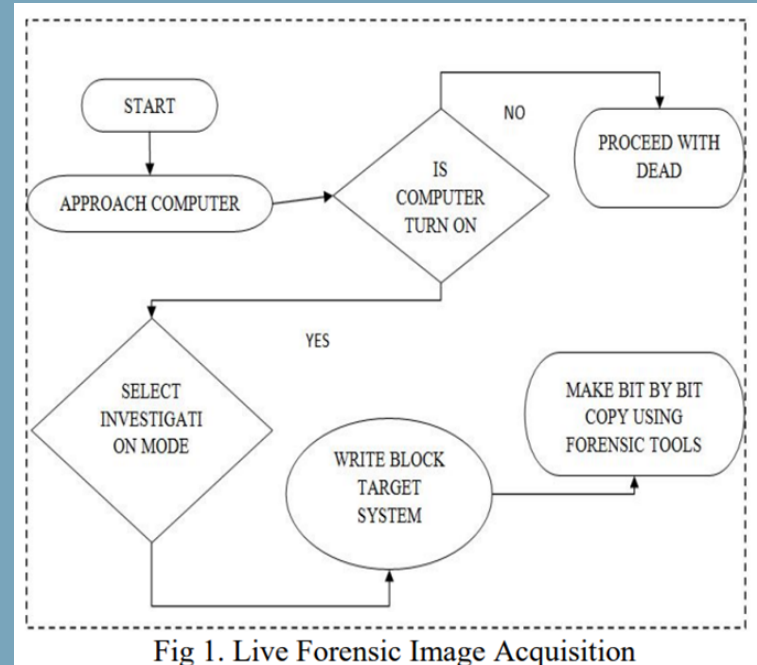
- No significant or insignificant changes to system and evidence
- No Legal questions to integrity
- Less time than live imaging



Imaging: Cloning/copying a physical storage for gathering evidence.
Pulling the plug was preferred but now is now subject to debate.

LIVE SYSTEMS aka Powered on/Running Machines:

- Evidence and data in RAM
- Unencrypted data
- Live imaging of RAM



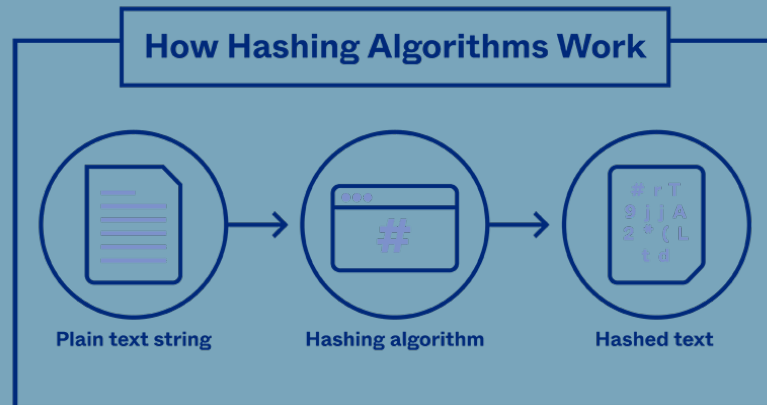
Hash Analysis

Used at any state of the digital forensics process to:

- Verify clone is exact replica of original device or evidence.
- Verify proper piece of evidence has been handed off.
- Integrity check throughout process.

Hash Values:

- Hash of original
- Hash of copy



Computer Science Major



picture

SHA256

c22699c05b52347fdf0046163537f3b7b8a55daad04674ad88d97aefe337cffa

Computer Science Major



picture - Copy

SHA256

c22699c05b52347fdf0046163537f3b7b8a55daad04674ad88d97aefe337cffa

Computer Science Major



picture edited

SHA256

ee03b0011a0b8b2a404329c8550b9eb90c483e64da34c7acd89ac76a0b7e6eec

Hash Analysis

Used at any state of the digital forensics process to:

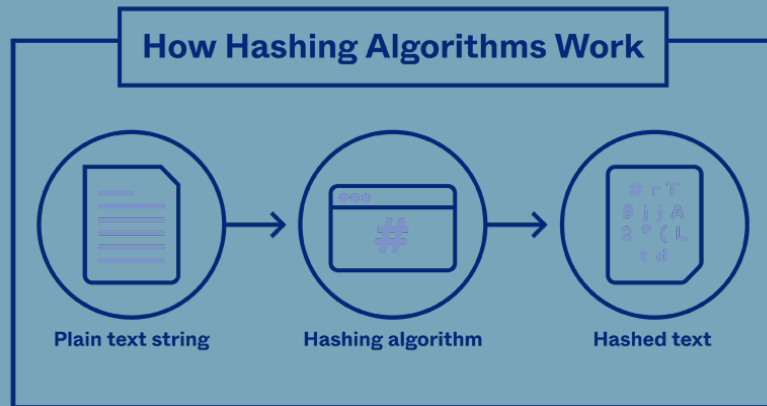
- Verify clone is exact replica of original device or evidence.
- Verify proper piece of evidence has been handed off.
- Integrity check throughout process.

Hash Values:

- Hash of original
- Hash of copy

Even smallest changes in **content** make differences in hash value.

Included in documentation and **vital** for getting evidence presented and used in court.



The Digital Forensics Process



Identification	Crime Scene & First Response, Search and Seizure
Evidence Collection & Preservation	Acquisition & Imaging, Live vs Dead Imaging, Hash Analysis
Analysis	Timestamps, File Metadata, Windows Registry
Documentation & Reporting	Chain of Custody, Final Reports & Expert Witness

Analysis

Identifying and examining vital evidence from acquired data and drawing conclusions to be presented in court.

Some things to look at:

- Time Stamps
 - MAC
 - Digital footprint
 - To put user behind keyboard linking other activity to timeframe
 - To pinpoint attacker by location and time of attack.
- File Metadata
- Windows Artifacts



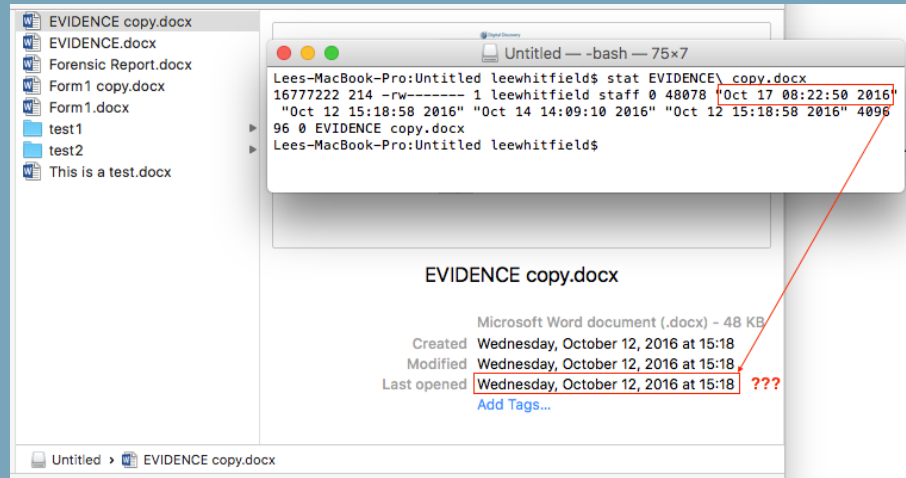
Time Stamps

Using MAC Times:

- Modified
- Accessed
- Created

Other Time Stamps:

- Email
- Browser History
- Link Files
- Registry



The Digital Forensics Process



Identification	Crime Scene, First Response, Search and Seizure
Evidence Collection & Preservation	Acquisition & Imaging, Live vs Dead Imaging, Hash Analysis
Analysis	Timestamps, File Metadata, Windows Registry
Documentation & Reporting	Chain of Custody, Final Reports & Expert Witness

Documentation & Report

- Stats and findings with interpretations
- Includes:
 - Chain of Custody
 - What was done to evidence, why, and by who
 - Verification Hashes
- **EVERYTHING DONE TO EVIDENCE SHOULD BE DOCUMENTED!**

ELEMENTS OF A DIGITAL FORENSIC REPORT

EXECUTIVE SUMMARY

Language: Non-technical

Purpose: High-level description of analysis findings in easily understood, non-technical language.

FINDINGS

Language: Technical

Purpose: Technical details of analysis to clearly describe the repeatable and defensible process. Include diagrams, charts, pictures.

APPENDED REPORTS

Language: Technical

Purpose: Further support the analysis of relevant information through presentation of highly detailed technical information, including evidence that can produce a tremendous amount of data such as email or chat message analysis.

CONCLUSION

Language: Non-technical

Purpose: Provide subjective analysis and expert opinions. Wrap up the analysis in a direct and concise manner.



DriveSavers • eDiscovery • Digital Forensics
800.440.1904 • DriveSavers.com

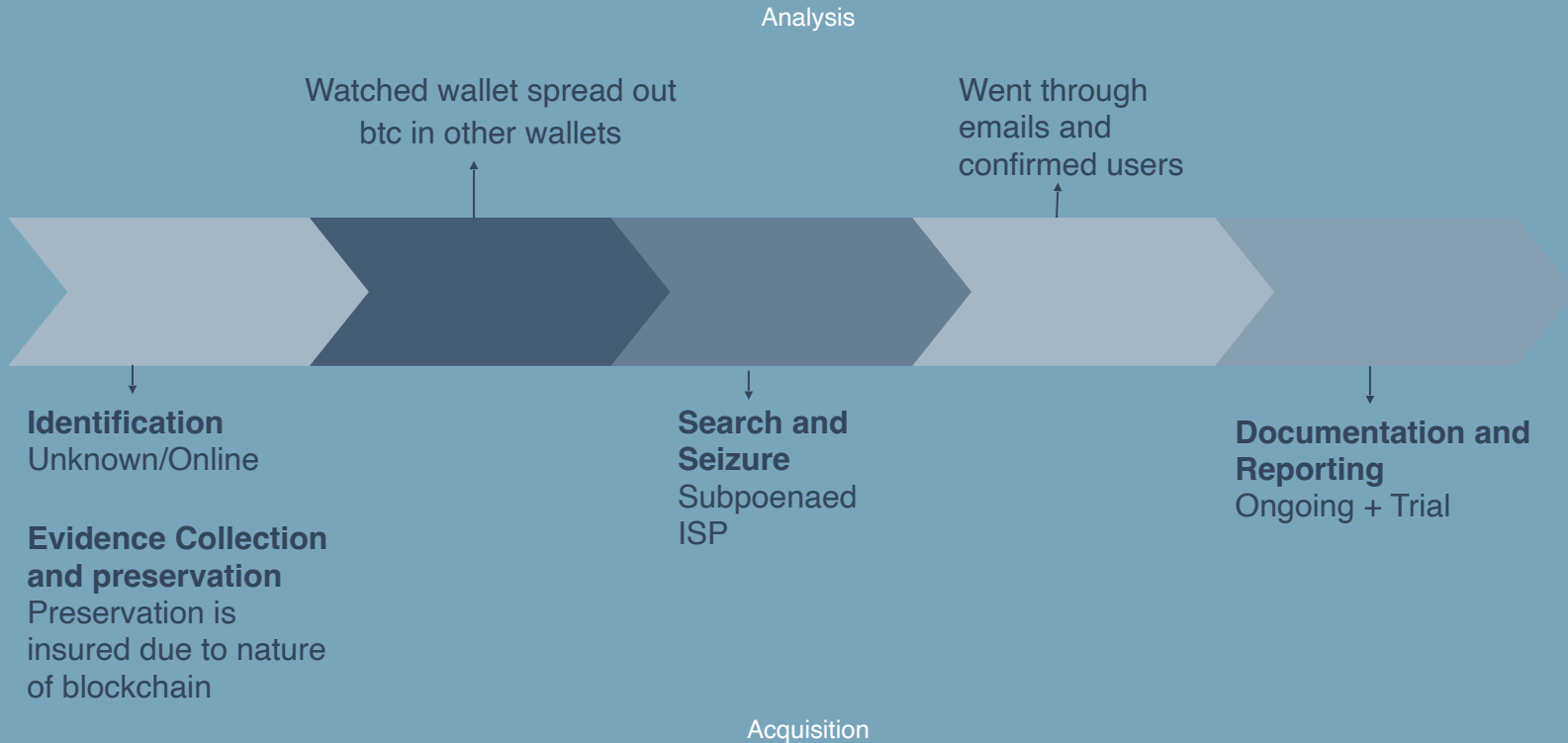
Expert Witness

Digital Forensic Scientist might be called in court as Expert Witnesses.

- To explain the process to the judge and jury in layman terms and give opinion
- To examine that the steps taken were valid and no mistakes were made by the forensics team in the case
- Must have no bias in the case



Bitcoin Crime Process



Anti-Forensic Techniques



Techniques used to hinder digital forensic investigations. I.e. compromise analyst's reports, delete evidence, obstruct log records of attacker's activities.

ENCRYPTION



ONION ROUTING

PROGRAM PACKERS

Compress/hide executable files from detection



STEGANOGRAPHY

Hidden digital content within non-secret digital content

DATA DESTRUCTION

Drive Wiping



CHANGING TIMESTAMPS

Change timestamps to escape investigation, hiding attacker's location and time of attack.





Steganography

The practice of hiding secret data/content in a different type of digital content files that are not secret in order to avoid being detected. ex. text, image, video, audio.

The secret data can be extracted from authenticated people with steganography tools to decode hidden messages.

- Often used together with encryption for extra layer.
- Malicious Payloads to bypass security and obscure trails.
- Hard for forensic experts to know when they are looking at one.
- Steganalysis

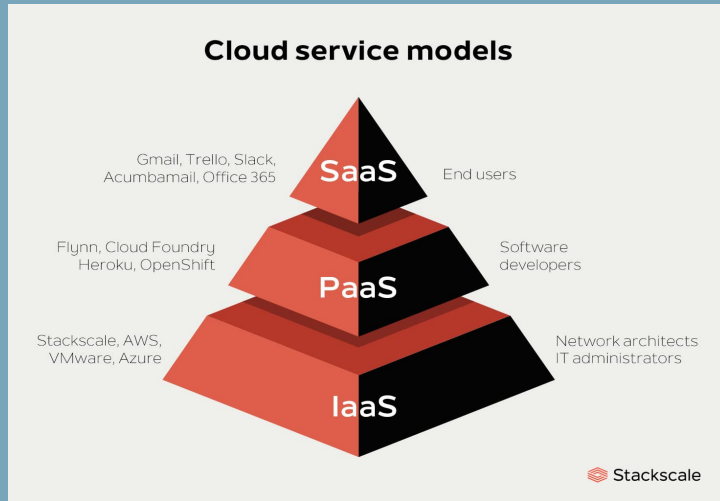
You've probably used Steganography! (Even if you didn't do the training or last weeks lab...)





STEGANOGRAPHY DEMO

Future of Forensics



- Cloud forensics
 - limited amount of backups
 - hides the data location from user
 - CSPs may not report the incident or cooperate
 - CSPs don't hire certified forensics investigators
 - Since all the data is with one CSP, if they have a failure all data is lost

Cloud Forensics challenges/ Process	Apply to Service model			Potential Solution	Ref	
	IaaS	PaaS	SaaS			
Identification						
Access to the evidence	✓	X	X	Eucalyptus framework OS and the security log	[41]	
	✓	X	X	a log-based model	[7]	
	✓	✓	X	Extraction of relevant status data	[15]	
	X	✓	X	A log management solution	[16]	
	✓	✓	X	An encrypted logging model	[14]	
Dependence on CSP & T	Trust Issue	✓	✓	X	Layers of Trust Model	[29]
	Data Acquisition	✓	✓	X	TrustCloud	[28]
	Compliance	✓	✓	✓	Cloud Management Plane	[42]
	Logs	✓	✓	✓	Service Level Agreement (SLA)	[11],
Lack of customer awareness	✓	✓	✓	--	[22]	
Volatile Data	✓	✓	X	Client Persistent Storage	[15]	
	✓	✓	X	A continuous synchronization API	[10]	

Future of Forensics

- Cloud forensics
 - Different service models have different issues
 - Ownership of multiple devices makes tracking difficult
 - Can't seize CSP's hard drives
 - Service Level Agreements (SLA) as a solution

- SSD and NAND storage
 - SSD's delete old data before overwriting

Summary

We talked about a lot today! Here are some of the most important parts:

- Digital Forensics is the investigative techniques and process for digital evidence.
- Digital Evidence != Just PC/Laptop Evidence
- **Computer Facilitated** (= computer as a tool) vs **Computer Based** (= computer as a target)
- 4 ACPO Principles among the most followed best practice for electronic evidence handling
- The digital forensic process includes **Identification** of evidence on the crime scene, search & seizure, **Evidence Collection** via Acquisition & Preservation & uses live/dead system imaging & hash analysis', **Analysis** of acquired data, **Documentation & Reporting**.
- **Steganography** is well known anti-forensic tool used to hide digital content in other forms of digital content

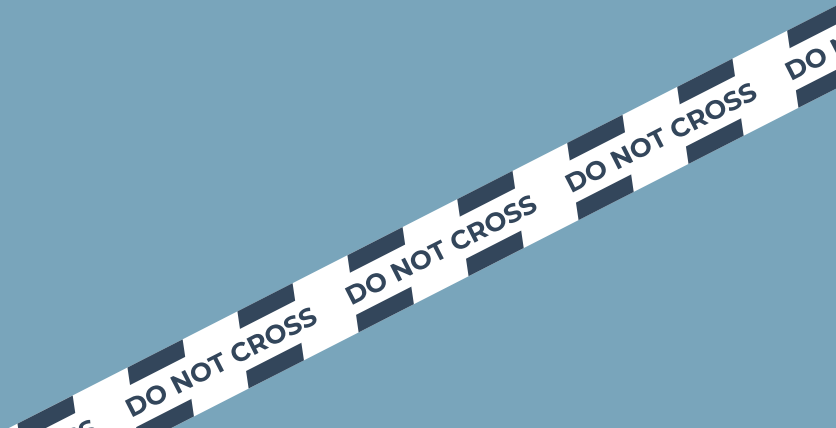




THANK YOU

Questions?

CREDITS: This presentation template was created by [Slidesgo](#), including icons by [Flaticon](#), and infographics & images by [Freepik](#).



REFERENCES

- Sammons, J. (2015). *The basics of Digital Forensics: The primer for getting started in Digital Forensics*. Syngress.
- <https://www.eccouncil.org/what-is-digital-forensics/>
- <https://onlinedegrees.unr.edu/blog/digital-forensics/>
- <https://ijcsit.com/docs/Volume%208/vol8issue3/ijcsit2017080331.pdf>
- <https://study.com/academy/lesson/first-responders-in-network-forensics-role-purpose.html#:~:text=A%20first%20responder%20in%20a,company%2Dissued%20desktop%20or%20laptop.>
- <https://www.geeksforgoeks.org/digital-evidence-preservation-digital-forensics/>
- <https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccd/check/art8.html>
- https://thesai.org/Downloads/Volume11No11/Paper_41-Analysis_of_Steganographic_on_Digital_Evidence.pdf
- <https://cisomag.eccouncil.org/6-anti-forensic-techniques-that-every-digital-forensic-investigator-dreads/>
- https://www.garykessler.net/library/fsc_stego.html
- <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.641.9370&rep=rep1&type=pdf>
- https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
- https://www.youtube.com/watch?v=ZUqzcQc_syE
- <https://www.wsj.com/articles/bitcoin-bitfinex-hack-crypto-laundering-morgan-lichtenstein-11644953617>
- <https://www.digitalforensics.com/blog/an-overview-of-web-browser-forensics/>
- <https://www.crimemuseum.org/crime-library/serial-killers/the-craigslist-killer/>
- <https://www.forensicscolleges.com/blog/forensics-casefile-craigslist-killer>
- <https://www.goodhousekeeping.com/life/entertainment/a28859869/btk-killer-dennis-rader/>
- <https://www.oxygen.com/sites/oxygen/files/styles/blog-post-embedded--computer/public/floppy-disk-killer.png?itok=N7OMjh3o>
- <https://www.wsj.com/articles/bitcoin-bitfinex-hack-crypto-laundering-morgan-lichtenstein-11644953617>
- <https://www.digitalforensics.com/blog/an-overview-of-web-browser-forensics/>
- <https://www.coindesk.com/policy/2022/02/14/federal-judge-releases-razzlekhans-orders-other-bitfinex-hack-laundering-suspect-to-remain-in-jail/>
- <https://archive.fo/tFc9D#selection-1143.165-1143.258>